Tutorial-AAI.zip

Enrico M.V. Fasanelli & Dael Maselli

Workshop CCR e INFN-GRID

La nuova strada dell'efficienza

Palau (Olbia) - 11 maggio 2009

Perché .zip

- Il Tutorial-AAI che organizziamo ogni anno, dura 4 giorni pieni
  - Teoria di Kerberos5 ed LDAP
  - Esercitazioni di laboratorio
  - È vero, ci sono anche i coffee-break ed i pranzi (le cene sono fuori dell'orario di lavoro) ma non facciamo mai meno di 7 ore piene di lavoro al giorno
  - Ed a giudicare dal grado di soddisfazione dei partecipanti (cibo a parte) il programma sembra essere ben strutturato

Time-zip?

- Se dai 4 giorni leviamo i coffee-break, le pause pranzo e le esercitazioni di laboratorio, rimangono comunque almeno 10 ore (in realtà sono un po' di più) di slides.
- Una possibile soluzione potrebbe essere sostituire il Fasanelli con qualcuno che faccia meno pause, ma anche così il rapporto di compressione sarebbe stato almeno 5:1

.zip o .snip?

- Snip è il suono delle forbici che tagliano qualcosa. Qualcosa dovrà essere sicuramente tagliato, ma non possiamo pensare ad un Tutorial-AAI fatto in 40 minuti che abbia senso, a meno di non “raccontare” quello che ci sarà da fare, e lasciare molto spazio alle domande.
- Questo è quello che abbiamo provato a fare, e speriamo di esserci riusciti.

Quattro passi
(non una passeggiata, ma…)

- Definire lo “schema”
- Popolare l’albero LDAP
- Implementare Kerberos5
- Configurare le applicazioni locali

Lo schema di INFN-AAI

- objectClass standard
  - person, inetorgPerson, posixGroup, ecc. ecc.

    + eduPerson (da Internet2/MACE)

    + SCHAC (SCHema for ACademia da TERENA)

    + infnPerson (da INFN-AAI con OID definiti secondo le regole)

    + objectClass locali già definite in alcune sedi, se compilate secondo le regole

Le regole

- Si parte da un “enrterprise number” assegnato da IANA, e che ha come prefisso `iso.org.dod.internet.private.enterprise (1.3.6.1.4.1)`
  - L’INFN ha il 10403 richiesto da Roberto Cecchini per la INFN-CA
  - Le assegnazioni fatte finora, sotto 10403 sono

```
.10403.1      INFN-AAI
.10403.5      LDAP di sede
.10403.5.1    Trieste
.10403.10     INFN-CA
.10403.10.1.6 INFN CA Certificate Policy and
              Certification Practice Statement
```

1.3.6.1.4.1.10403.1 INFN-AAI

- Attributi

  `.10403.1.1  INFN-AAI Attributes`

- Classi di Oggetti

  `.10403.1.2  INFN-AAI objectClasses`

- Altro

  `.10403.1.10 INFN-AAI Entitlements (valori che dipendono dalle applicazioni e che servono ad esse per le autorizzazioni “implicite” ossia quelle demandate alla AAI)`

infnPerson

```
objectClasses: ( 1.3.6.1.4.1.10403.1.2.1
  NAME 'infnPerson'
  SUP top AUXILIARY
  MUST ( infnPersonUUID )
  MAY  ( infnPersonCF $
         infnPersonContractProfile $
         infnPersonContractType $
         infnPersonContractStart $
         infnPersonContractEnd $
         infnPersonRoleDN $
         infnPersonPrimaryAccountDN $
         infnCertSubjectDN $
         infnAccountKerberosPrincipal )
  X-ORIGIN 'INFN AAI' )
```

infnCertSubjectDN

```
attributeTypes: (1.3.6.1.4.1.10403.1.1.7
  NAME 'infnCertSubjectDN'
  DESC 'DN del Subject del Certificato X.509'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  X-ORIGIN 'INFN AAI' )
```

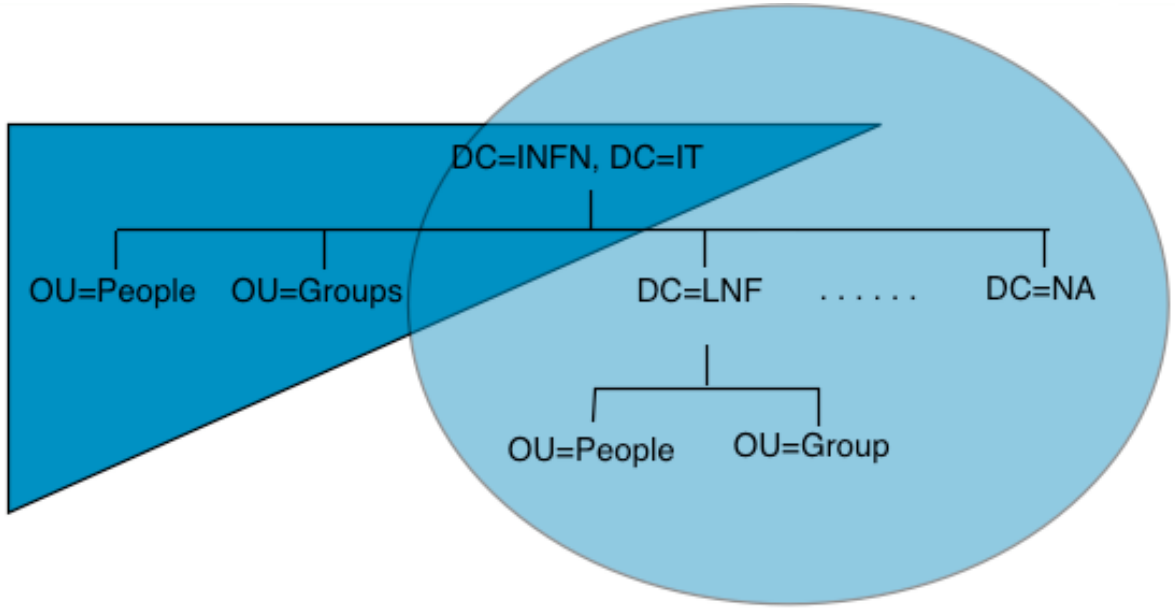
- SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  - ‘DN’ syntax definita nell’RFC 2252 LDAP(v3) Attribute Syntax Definitions

Quattro passi
(non una passeggiata, ma…)

- Definire lo “schema”
- Popolare l’albero LDAP
- Implementare Kerberos5
- Configurare le applicazioni locali

L’albero INFN-AAI

- Due parti logiche
  - Informazioni relative alle persone sotto DC=INFN,DC=IT
  - Alberi di “sede”



Popolare l'albero LDAP

- "Merge" tra informazioni presenti in
  - LDAP di DataWeb
  - protoAAI
  - Informazioni locali
- Via software opportunamente scritto (GOVA)
- Possibili e probabili eccezioni da gestire "manualmente" (sempre via GOVA)

GOVA.fillTree

- Prende in pasto un file formato LDIF contenente le informazioni relative all'utente (username, uid, gid, gecos, shell, e-mail, ecc. ecc.)
- Associa tale utente alla persona presente nell'LDAP di DataWeb, e ne arricchisce le informazioni (infnPersonUUID, ecc. ecc.)
- Popola automaticamente l'albero LDAP o richiede intervento manuale
  - Omonimie
  - Mancanza della registrazione della persona

Quattro passi
(non una passeggiata, ma…)

- Definire lo “schema”
- Popolare l’albero LDAP
- Implementare Kerberos5
- Configurare le applicazioni locali

Kerberos5

- Installare e configurare un KDC master ed un paio di KDC slave è un'attività ben descritta nelle slides dei Tutorial-AAI (quelli non zippati)
- Il problema vero è far diventare le utenze di una sede dei principal Kerberos senza dover chiedere agli utenti (possono essere varie centinaia) di effettuare delle operazioni.
  - Plug-in di FDS per popolare i vari KDC
- Ovviamente c'è poi da configurare tutti i client…

Quattro passi
(non una passeggiata, ma…)

- Definire lo “schema”
- Popolare l’albero LDAP
- Implementare Kerberos5
- Configurare le applicazioni locali

Un esempio di applicazione

Configurazione del login su linux RedHat

```
# authconfig --enableshadow --enablemd5 --enableldap \
--ldapserver=dsa.sede.infn.it \
--ldapbasedn="ou=People, dc=sede, dc=infn, dc=it" \
--enableldapauth --enableldaptls --enablecache \
--disablenis --enablekrb5 --krb5realm  SEDE.INFN.IT \
--krb5kdc kdcs1.sede.infn.it --krb5adminserver kdca.sede.infn.it

# cp INFN_CA.crt /etc/openldap/
# echo "TLS_CACERT /etc/openldap/ca.crt" >> /etc/ldap.conf
# echo "TLS_CACERT /etc/openldap/ca.crt" >> /etc/openldap/ldap.conf
```

Un esempio di applicazione

Sendmail.mc

```
define(`confLDAP_DEFAULT_SPEC', ` -h ds.sede.infn.it -b ou=People,
        dc=sede, dc=infn, dc=it')
LDAPROUTE_DOMAIN(`sede.infn.it')
FEATURE(`ldap_routing',
   `ldap -1 -T -v mailHost -k
   "(&(objectClass=mailRecipient)
   (|(mail=%0)(mailalternateaddress=%0)))"`,
   `ldap -1 -T -v mailRoutingAddress -k
   "(&(objectClass=mailRecipient)(uid=%s))"` ,
    `bounce' ) dnl
```

Domande ma principalmente discussione

Enrico M.V. Fasanelli

Dael Maselli

Claudio Bisegni